CHI
controlla
CHAT
controll?

COMBATTERE
LA PEDOPORNOGRAFIA
NEL 1984

APPROFONDIMENTI

CHAT CONTROLL CHI CONTROLLA?

COMBATTERE LA PEDOPORNOGRAFIA NEL 1984

DI REDAZIONE

CHAT CONTROL: COS'È E PERCHÉ È UN PROBLEMA

Il Chat Control (nome all'anagrafe "Regulation to Prevent and Combat Child Sexual Abuse") è un regolamento UE in cantiere ormai da diversi anni (2022), ma che è recentemente salito agli onori della cronaca visto che oggi 14 ottobre è stato votato (con esito negativo) dal Consiglio Europeo.

Come suggerisce il nome, lo scopo dichiarato è combattere la condivisione di materiale pedopornografico e l'adescamento di minori sul web. Ma se l'obiettivo è nobile, le modalità previste dal regolamento puzzano di marcio.

Le autorità statali europee (e non) mostrano da diversi anni una certa allergia nei confronti delle prassi di sicurezza e privacy delle piattaforme di messaggistica istantanea, in particolare a causa della famigerata end-to-end encryption (E2EE). Quando inviamo un messaggio su WhatsApp, Signal e compagnia cantante, il nostro telefono usa una chiave crittografica[1] per celare i contenuti del messaggio; il messaggio criptato viene salvato sui server della piattaforma e inoltrato al destinatario, che con la sua chiave sul suo telefono può decriptare il messaggio e leggerne il contenuto.

Questo simpatico sistema garantisce che quand'anche la sig.ra Postale bussasse agli uffici del sig. Signal chiedendo di accedere ai dati di una chat, Signal potrebbe serenamente consegnare i dati richiesti e farsi una risata, con la certezza che la sig.ra Postale non sarebbe in grado di leggere assolutamente niente. Punto fondamentale: lo stesso vale per chiunque ottenga tali dati in maniera illecita, ragion per cui la E2EE è oggi il principale deterrente contro azioni di hacking delle piattaforme di messaggistica e concorre a garantire privacy e sicurezza all3 utenti.

Con il Chat Control l'UE vuole obbligare le piattaforme che operano in Europa a modificare le proprie applicazioni in modo da includere un sistema di controllo direttamente sui telefoni dell3 utenti: i messaggi verrebbero inviati a dei server (statali e/o privati) per essere controllati da IA e/o persone prima di essere criptati. Questo vuol dire che i nostri messaggi viaggerebbero attraverso la rete e verrebbero conservati su server in chiaro, senza le garanzie di protezione dell'E2EE.

Bocciatura, possibili modifiche e perché sarà ancora un problema

Per le ragioni di cui sopra, il Chat Control oggi non passerà al Consiglio dell'UE: le pesanti critiche di praticamente chiunque ne capisca qualcosa, le controversie generate da uno strumento simile in Regno Unito[2], la pressione dei garanti della privacy europei e in ultimo il veto della Germania hanno avuto l'effetto di avviare una riscrittura del testo con lo scopo di introdurre più paletti tecnici e un maggior coinvolgimento della magistratura nell'approvazione del suo utilizzo.

Anche se il Chat Control è stato bocciato c'è poco da stare allegr3: i legislatori UE sembrano determinati ad ottenere una forma di controllo preventivo[3] delle chat private dell3 cittadin3 - nonostante i reiterati pareri negativi di associazioni che si occupano di difesa dell3 minori, garanti della privacy, aziende tech e Nazioni Unite, secondo cui il Chat Control rischia di avere l'unico effetto di sottrarre risorse agli strumenti già esistenti di lotta alla pedopornografia. E al di là delle possibili modifiche al testo, la crittografia delle chat resta un insormontabile ostacolo tecnico che le istituzioni dovranno in qualche modo forzare.

PIZZA MAFIA AND DIGOSSINO

L'Italia, inizialmente tra gli Stati più favorevoli alla misura, è oggi nella lista degli "indecisi". Che potrebbe anch sembrare un dato positivo, se non fosse che non lo è.

In primis, c'è da considerare che il governo di

Meloni & Co. vede la sua autonomia d'azione limitata dalle recenti agitazioni di piazza in sostegno al Popolo palestinese: in un contesto di esacerbazione del conflitto ideologico e di alta volatilità del consenso, inevitabilmente la gestione interna del dissenso guadagna importanza e le ricadute di una misura liberticida e mediaticamente attenzionata come questa possono essere imprevedibili.

E secondariamente: perché incagliarsi nelle lungaggini burocratiche degli organi decisionali europei quando si può tranquillamente ricorrere a strumenti nostrani, saldamente nelle mani della destra di governo?

Plot twist: in Italia il Chat Control esiste ed è utilizzato dalle forze di polizia dai primi anni del 2000, pur senza un quadro legislativo che ne regolasse l'uso. Dal punto di vista tecnico è semplice quanto brutale: malware "trojan horse"[4]. Nelle sue ultime, più efficaci versioni, era sufficiente scaricare uno sticker nella chat di un contatto fidato (e spesso inconsapevole) per installare il virus, che da quel momento in poi garantiva agli sbirri totale controllo da remoto del telefono vittima.

Tutto ciò ha ovviamente creato un certo scalpore per l'assenza di un recinto legale che ne regolamentasse l'uso, per cui è stato prontamente inserito in una cornice istituzionale dall'ex-ministro Orlando nel 2017, prevedendolo come regolare strumento d'indagine per fattispecie di reato che rientrino nelle categorie del terrorismo e dell'associazione a delinquere.

CHE GRAN COINCIDENZA che si stia discutendo proprio in questo periodo il DDL Gasparri, che mira a equiparare il sostegno alla Popolazione palestinese all'antisemitismo, rendendolo penalmente perseguibile.

E CON QUALE INCREDIBILE TEMPISMO arriva la "tregua" imposta da Trump su Gaza, che i governi alleati del sionismo stanno usando come trappola comunicativa per dipingere ogni pro Pal come un3 potenziale terrorista.

If it looks like a duck[5]...

Insomma per tirare queste somme non serve un computer quantistico: se l'accentramento dei nostri dati nelle mani di pochi, grandi e non disinteressati attori del panorama tecnologico configura una seria quanto subdola minaccia alla nostra privacy, l'interesse a metterci becco di alcune istituzioni europee e statali fa preoccupare ancor di più: ogni giorno il muro tra distopia orwelliana e realtà sembra farsi più sottile, ma non è un sogno. Viviamo un momento storico di riarmo, guerre e genocidi, in cui l'inasprimento delle misure che riguardano la "sicurezza" e "l'antiterrorismo" dovrebbero farci interrogare a fondo sulla pericolosità della nostra libertà di esprimerci per il potere costituito.

Il consiglio pratico:

Se sei un3 utente medi3, rifuggi per quanto possibile dai servizi di Big Tech come Google, Amazon, Meta e altre compagnie che oltre a rappresentare un baratro etico hanno anche tendenze collaborazioniste con l'amministrazione Trump. Una transizione graduale non è troppo impegnativa e su Reddit si trova tutto lo scibile umano sul tema;

Se sei un3 utente tecnicamente preparat3 o fai parte di un'organizzazione che ha gli strumenti e il know-how necessari, considera di iniziare a fare self-hosting per i servizi che utilizzi e contribuisci a diffondere consapevolezza informatica e prassi di internet libero;

Visita fightchatcontrol.eu per rimanere informat3 sugli sviluppi.

[1] Queste chiavi sono tali per cui un PC impiegherebbe più di qualche miliardo di anni per calcolarle, anche se va detto che i neonati computer quantistici consentirebbero di svolgere lo stesso lavoro in poche ore

[2] L'applicazione dell'Online Safety Act 2.0 ha portato alla rimozione di post contro il governo Starmer o contro Joe Biden

[3] "Preventivo" è la parola chiave: le intercettazioni delle comunicazioni telematiche sono già possibili in caso di indagini penali, ma il Chat Control sarebbe, in quanto forma di controllo preventivo, costantemente attivo sulle chat di tutt3.

[4] "Trojan horse" è un tipo di malware che prende il nome dal famigerato cavallo di Troia: viene installato nel dispositivo mascherato da file innocuo e da quel momento consente all'intruso di controllare a distanza qualunque file, microfoni, videocamere e così via, senza che l'utente ne sia consapevole.

[5] Il riferimento è al "duck test", che enuncia: "if it looks like a duck, swims like a duck and quacks like a duck, then it probably is a duck" ("Se ha l'aspetto di una papera, nuota come una papera e starnazza come una papera, probabilmente è una papera"